RISIKO OPERASI

Operasi institusi kewangan kekal berdaya tahan

Memelihara daya tahan operasi dan siber institusi kewangan terus menjadi salah satu bidang tumpuan utama bagi BNM. Pada separuh kedua tahun 2024, kerugian kewangan akibat risiko operasi yang dilaporkan oleh institusi kewangan kekal rendah, merangkumi hanya 0.03% daripada jumlah modal sistem perbankan (ST1 2024: 0.05%; ST2 2023: 0.03%). Institusi kewangan terus memantau gangguan operasi, terutamanya berikutan landskap ancaman siber yang semakin meningkat.

Sepanjang tempoh ini, beberapa insiden siber dilaporkan oleh industri, meskipun kebanyakannya melibatkan tahap keseriusan yang rendah. Jumlah serangan penafian perkhidmatan teragih (*distributed denial of service*, DDoS) mencatatkan sedikit peningkatan, seterusnya mengakibatkan ancaman yang berterusan kepada ketersediaan perkhidmatan dalam talian oleh institusi kewangan. Institusi kewangan telah menyediakan pelan kesinambungan perniagaan (*business continuity plans*, BCP) yang sewajarnya bagi memastikan kesiapsiagaan mereka untuk bertindak balas dan pulih daripada insiden siber serta meminimumkan gangguan operasi. BNM juga terus memantau landskap ancaman siber secara proaktif dan mempertingkatkan langkah penyeliaan untuk membanteras dan menangani ancaman yang semakin meningkat. Langkah ini termasuk mengemas kini keperluan dasar bagi menangani risiko baharu, serta menjalankan kajian bersasar untuk menilai keupayaan institusi kewangan bertindak balas terhadap insiden siber.

Hutang teknikal[34] dan keselamatan[35] (*technical and security debt*) boleh menyumbang kepada peningkatan tahap mudah terjejas industri kewangan terhadap ancaman siber. Sehubungan dengan itu, BNM terus menggesa institusi kewangan supaya memperkukuh pertahanan berbilang lapisan mereka. Usaha ini termasuk memastikan proses perniagaan yang mengalami pendigitalan pantas disertai dengan sumber dan kepakaran yang mencukupi. Hal ini adalah untuk menguruskan risiko pelaksanaan dan mengekalkan daya tahan operasi secara berterusan untuk menghadapi perkembangan dalam risiko teknologi dan siber. Perbelanjaan tahunan institusi kewangan dalam bidang teknologi maklumat (*information technology*, IT) telah meningkat dalam tempoh beberapa tahun kebelakangan ini, dengan kadar pertumbuhan tahunan terkompaun (*compound annual growth rate*, CAGR) sebanyak 22% bagi tempoh tiga tahun yang lepas. Yang ketara, perbelanjaan IT terus mewakili bahagian yang semakin besar daripada jumlah perbelanjaan tahunan keseluruhan (2024: 23.3% daripada perbelanjaan tahunan; 2023: 19.1%; 2022: 18.7%). Pertambahan ini mencerminkan kepentingan strategiknya yang semakin meningkat bagi institusi kewangan. Sebahagian besar perbelanjaan ini diperuntukkan bagi:

- melaksanakan usaha penyegaran semula teknologi, seperti penggantian serta penggunaan penyelesaian keselamatan siber yang lebih baik;
- mempertingkatkan pengurusan infrastruktur IT dan pemantauan rangkaian;
- memperkukuh perkhidmatan risikan ancaman dan pemantauan keselamatan; dan
- meningkatkan latihan kepada kakitangan IT dan keselamatan siber serta fungsi pemantauan dan kawalan utama bagi menguruskan trend dan risiko siber yang baharu.

Peningkatan perbelanjaan IT tahunan ini didorong oleh usaha menaik taraf infrastruktur pusat data bagi memastikan daya tahan operasi pada waktu puncak. Peningkatan ini juga berikutan inovasi produk secara pesat yang turut menambah kerumitan operasi infrastruktur IT institusi kewangan. Beberapa bank telah melancarkan program jangka panjang untuk memodenkan sistem IT mereka. Program ini merangkumi pembinaan semula infrastruktur rangkaian dan pelayan untuk memastikan kawalan berpusat, ketangkasan dan fleksibiliti yang lebih baik. Sesetengah bank terus mempertingkatkan kecekapan operasi IT, misalnya melalui penggunaan penyelesaian keselamatan berasaskan awan (*cloud-based security solutions*). Bank-bank utama secara amnya memperuntukkan perbelanjaan modal untuk menaik taraf sistem teras yang mendekati akhir hayat perkhidmatannya, memastikan persekitaran IT yang selamat serta meningkatkan kapasiti sistem dan infrastruktur sandaran. Selain itu, institusi kewangan pembangunan serta penanggung insurans dan pengendali takaful turut menaik taraf keupayaan pusat data bagi memastikan pemulihan perkhidmatan yang pantas pada waktu puncak. Langkah ini diambil sejajar dengan kehendak pengawalseliaan untuk memastikan ketersediaan perkhidmatan yang berterusan bagi mengekalkan keyakinan orang ramai. Kesemua langkah ini juga selaras dengan penerapan piawaian dan rangka kerja antarabangsa

[34] Hutang teknikal merujuk kompromi dalam bidang IT apabila pembetulan, naik taraf atau penambahbaikan ditangguhkan atau dilaksanakan secara kurang optimum berikutan kekangan tarikh akhir atau belanjawan. Hal ini menyebabkan peningkatan kos dan usaha tambahan pada masa hadapan bagi menangani isu yang semakin bertambah.

[35] Hutang keselamatan pula merupakan sebahagian daripada hutang teknikal yang memberikan tumpuan pada aspek keselamatan. Keadaan ini berlaku apabila amalan dan protokol keselamatan terbaik diberikan kurang keutamaan untuk memastikan kemajuan yang lebih pantas atau keutamaan tertumpu pada bidang lain. Dari masa ke masa, hal ini menyebabkan kelemahan dalam persekitaran sistem terkumpul secara beransur-ansur, menjadikan sistem lebih sukar untuk dipertahankan serta meningkatkan kos dan risiko pada masa hadapan.

yang lebih meluas bagi mengukuhkan pengurusan keselamatan maklumat.[36]

Sebagai sebahagian daripada usaha yang dipertingkatkan bagi memastikan BCP institusi kewangan lebih menyeluruh dan meliputi pelbagai senario, bank-bank dikehendaki membangunkan ujian BCP yang lebih mantap dan bersepadu. Langkah ini bertujuan memastikan kesinambungan perkhidmatan dan operasi bank yang sangat penting dalam persekitaran yang semakin kompleks dan saling bergantung.

Institusi kewangan telah mengenal pasti usaha menguruskan ancaman siber, memastikan pematuhan terhadap keperluan pengawalseliaan serta membendung taktik kejuruteraan sosial oleh penjenayah penipuan sebagai keutamaan teras dalam menguruskan risiko operasi pada tahun 2025.[37] Hal ini berikutan peningkatan dalam modus operandi ancaman terhadap industri serta jangkaan untuk memastikan institusi kewangan sentiasa mampu menyediakan perkhidmatan digital yang selamat dan tersedia. Risiko-risiko ini diberikan keutamaan kerana terus berkembang seiring dengan landskap sektor kewangan yang sentiasa berubah (Gambar Rajah 1.2).

Selanjutnya, bagi menggerakkan pemantauan risiko operasi sistem kewangan secara lebih menyeluruh dan sistematik, BNM telah menambah baik pelaporan risiko operasi berpusat menerusi sistem Pelaporan Risiko Operasi (Operational Risk Reporting, ORR) untuk mengumpulkan lebih banyak data berkaitan risiko operasi. Sistem ORR menyokong pelaporan dan penilaian insiden risiko operasi kepada BNM serta memantau tindak balas insiden oleh institusi kewangan. Sistem ini merangkumi pelaporan insiden berkaitan penipuan, amalan dan gangguan operasi dalam institusi kewangan. Dengan peningkatan interaksi antara operasi perbankan yang sangat penting dengan ekosistem pembayaran, penyertaan entiti sistem pembayaran yang dikawal selia dalam sistem ORR baru-baru ini juga akan memberikan gambaran yang lebih menyeluruh mengenai dedahan dan daya tahan keseluruhan sektor kewangan terhadap risiko operasi.

Gambar Rajah 1.2: Risiko Operasi Utama dan Tindakan Mitigasi

Ancaman Siber	Jenayah siber sebagai perkhidmatan semakin berleluasa, ditambah pula dengan serangan yang dipacu AI, menjadikan ancaman siber lebih rumit dan canggih.	• Syarat yang lebih ketat dalam pengurusan risiko siber untuk pihak ketiga dan rantaian bekalan. • Meningkatkan kesiapsiagaan dan tindak balas terhadap insiden siber melalui latihan simulasi serangan siber di seluruh industri. • Perkongsian risikan ancaman siber yang lebih meluas melalui FinTIP.
Ketidakpatuhan Pengawalseliaan	Peraturan yang semakin ketat dan peningkatan dalam penelitian orang awam meningkatkan permintaan terhadap institusi kewangan untuk memastikan pematuhan, terutamanya dalam pelaporan pengawalseliaan serta memastikan ketersediaan perkhidmatan dalam talian.	• Libat urus secara berkala dengan industri bagi memastikan penyelarasan serta menggalakkan perkongsian amalan terbaik. • Pengukuhan fungsi kawalan dalaman bagi mengenal pasti dan membetulkan jurang pematuhan mengikut masa yang ditetapkan. • Pengawasan yang lebih ketat terhadap pengurusan risiko IT oleh institusi kewangan.
Kejuruteraan Sosial	Modus operandi penipuan yang semakin berkembang, seperti penipuan aplikasi palsu, semakin licik memperdaya pelanggan supaya mendedahkan butiran perbankan atau maklumat sensitif mereka yang lain.	• Meningkatkan kesedaran orang ramai tentang modus operandi penipuan melalui pelbagai saluran komunikasi. • Kerjasama merentas sektor melalui National Fraud Portal (NFP) bagi mempercepat tindak balas terhadap penipuan. • Meningkatkan keupayaan pengesanan penipuan oleh institusi kewangan dengan mengesan dan menyekat transaksi yang mencurigakan.
Kesilapan Manusia	Peningkatan jumlah transaksi serta perubahan dalam proses dalaman selepas pendigitalan meningkatkan risiko kesilapan dan kecuaian operasi.	• Kawalan dalaman yang lebih ketat serta prosedur operasi standard (SOP) yang dikemas kini lebih kerap bagi menunjukkan perubahan proses. • Pembinaan keupayaan pekerja yang berterusan bagi mengurangkan kecuaian operasi. • Penggunaan sistem analitik untuk mengesan dan mencegah kesilapan berulang.
Gangguan Perniagaan	Pergantungan yang lebih besar pada teknologi, sistem dan penyedia perkhidmatan pihak ketiga (TPSP) mendedahkan institusi kewangan pada risiko gangguan perkhidmatan dan kegagalan sistem.	• Pemantauan yang lebih rapi terhadap prestasi sistem penting dan potensi ancaman, termasuk perkhidmatan penting yang disediakan atau disokong oleh TPSP. • Pelan kesinambungan perniagaan dan pemulihan bencana yang kukuh serta diuji secara berkala bagi memastikan keberkesanannya.

Sumber: Bank Negara Malaysia

[36] Piawaian dan rangka kerja ini termasuk ISO/IEC 27001 Information Security Management System (ISMS), US National Institute of Standards and Technology (NIST) Cybersecurity Framework dan Payment Card Industry Data Security Standard (PCI DSS).

[37] Berdasarkan Emerging Operational Risk Survey 2024/2025 yang dijalankan oleh BNM.

Sistem pembayaran dan penyelesaian mengekalkan tahap ketersediaan yang tinggi.

Sistem Pemindahan Dana dan Sekuriti Secara Elektronik Masa Nyata (Real-time Electronic Transfer of Funds and Securities, RENTAS) dan sistem pembayaran runcit (*retail payment system*, RPS) utama terus mengekalkan tahap daya tahan operasi dan ketersediaan sistem yang tinggi sepanjang separuh kedua tahun 2024.

Tiada insiden operasi atau siber yang signifikan berlaku dalam tempoh ini. Sebagai sebahagian daripada usaha berterusan untuk mengekalkan daya tahan sistem, penambahbaikan selanjutnya telah dilaksanakan dalam pengurusan kesinambungan perniagaan RENTAS dan RPS utama bagi memperkukuh langkah pemulihan sistem bagi menghadapi kemungkinan berlakunya serangan siber tahap ekstrem. Perincian lanjut mengenai pemantauan perkhidmatan pembayaran boleh didapati melalui bab "Menggalakkan Pembayaran dan Perkhidmatan Kiriman Wang yang Selamat dan Cekap" dalam Laporan Tahunan BNM 2024.